Perm Winter School 2018

Scaling Blockchain

Mihail Nikulin, Co-founder & CTO, Lykke

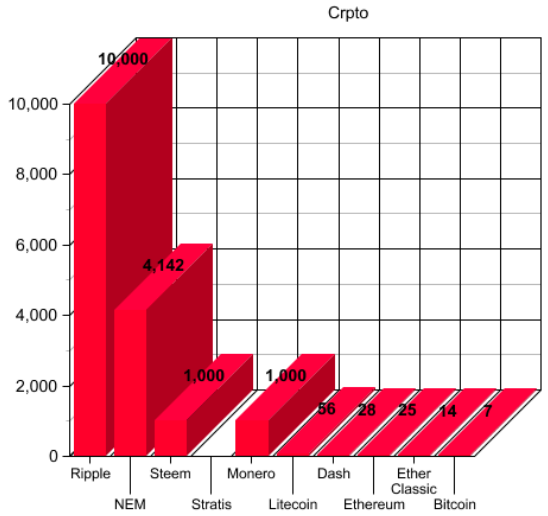
Bitcoin as benchmark

1. Bitcoin is the first Blockchain
2. Most known blockchain
3. Biggest capitalization
4. Crypto assets are nominated in Bitcoin mostly

Scaling blockchain is not something new

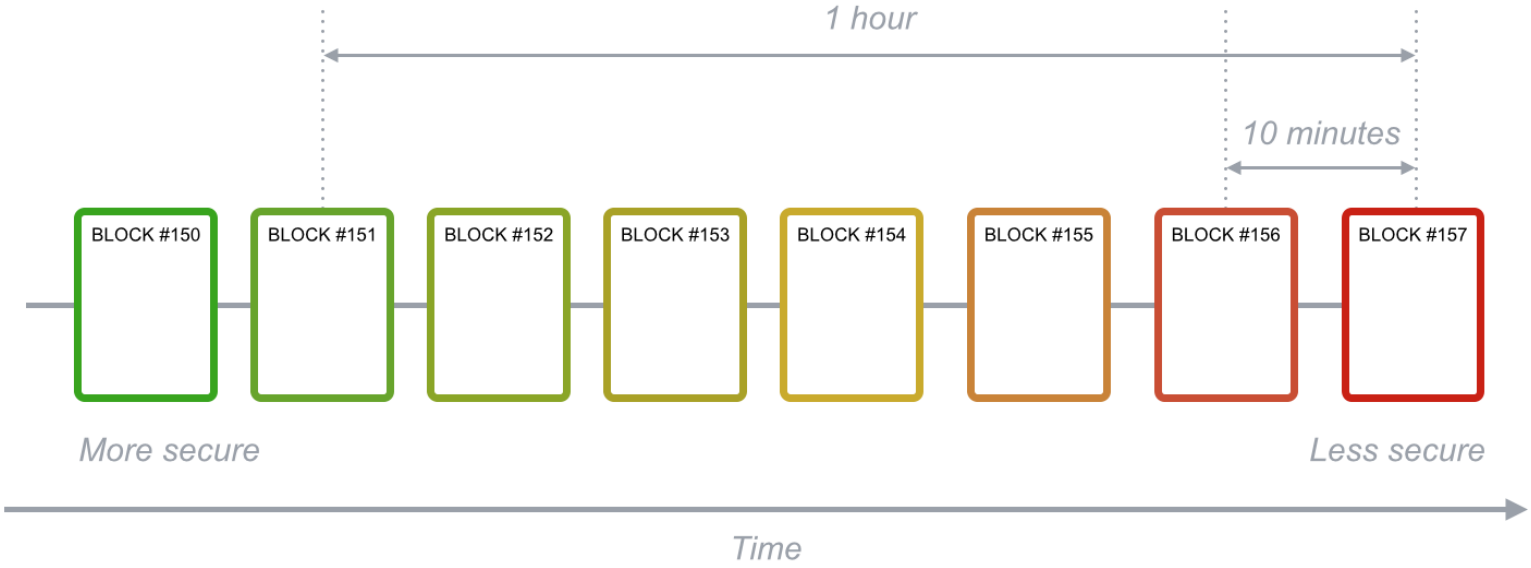
VISA is capable to handle up to 50k transactions per second

1. Bitcoin 7 txn per second, 12k nodes
2. Ethereum 25 txn per second, 26k nodes
3. Monero 1000 txn per second
4. Ripple 1000 txn per second



And then he said “Lightning network will scale Bitcoin”

Why Bitcoin Blockchain is Not Scalable



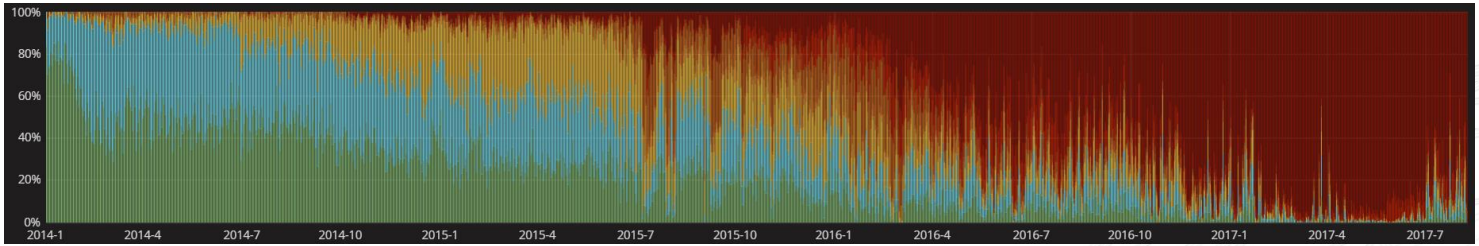
Why Bitcoin Blockchain is Not Scalable

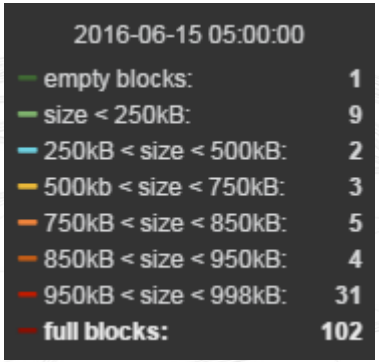
1 Mb block size

7 transactions per second (250 bytes/transaction)

220 mln transaction per year(!)

Not enough for city, let alone the world





Block size problem

1 Billion transaction per day requires:

1.6 GB blocks

87 Tb/Year

1 Billion people doing 2 transaction per day:

- 24 GB block
- 3.5 Tb/Day
- 1.27 Pb/Year

Bigger block = Centralization

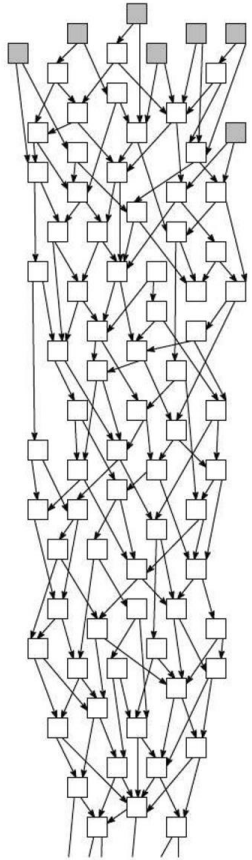
- Very few full nodes
- Very few miners
- De facto inability to validate blockchain

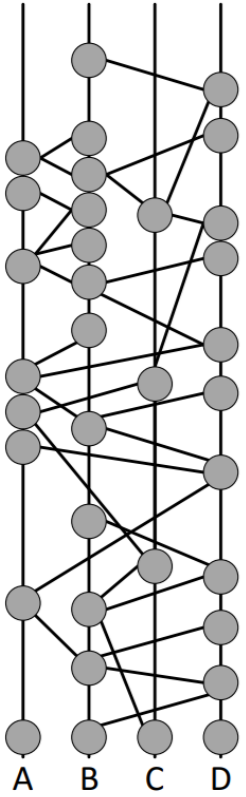
Lightning Network (state channel)

1. Allows to settle up to millions transactions per second
2. No need to settle each single transaction on the blockchain
3. Almost as secure as on-chain transactions
4. Private peer-to-peer communications inside the state channel
5. Currently the only solution for scaling Bitcoin

Alternative approaches to scale blockchain

1. PoS
2. Sharding
3. Directional Acyclic Graph Ledgers (IOTA, Hashgraph)
4. …





Why does Lykke consider the scalability problem

1. Lykke DNA is semi-decentralized exchange (combines speed and direct ownership)
2. Lykke does not want to take possession on the client’s money
3. Super fast centralized matching requires trust
4. Immediate settlement allows to minimize custodian risks for clients

Lykke operational mode

1. June 2016- June 2017 every single trade was recorded on the blockchain as atomic swap
2. 1st of June 2017 Lykke switched to the Lightning Network model

Lightning network is a silver bullet?

Single on-chain transaction

Alice’s wallet

Transfer requires to pay fees

Bob’s wallet

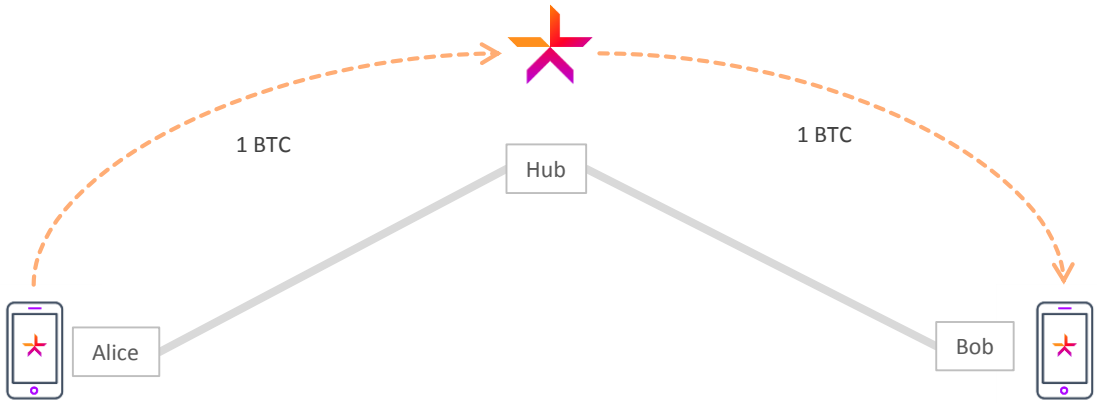
What is a payment channel?

Alice + Bob micropayment channel (state channel)

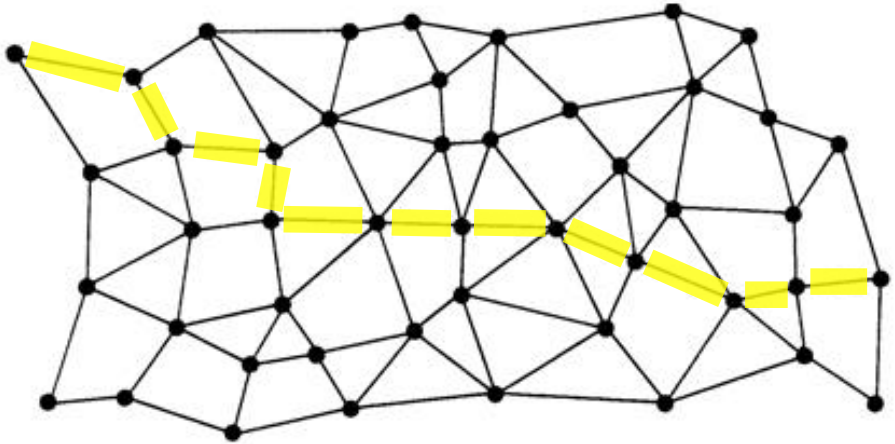
Alice’s wallet

Bob’s wallet

LN Liquidity Hub

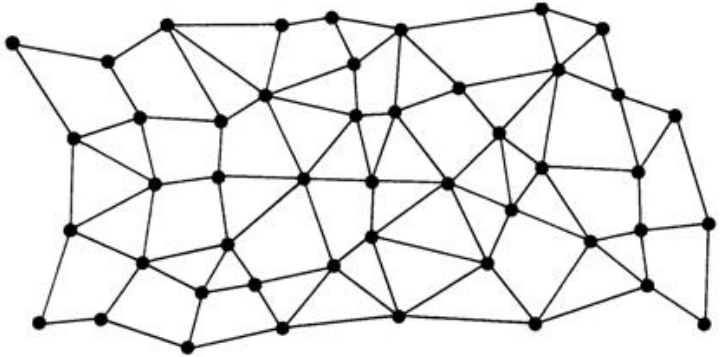


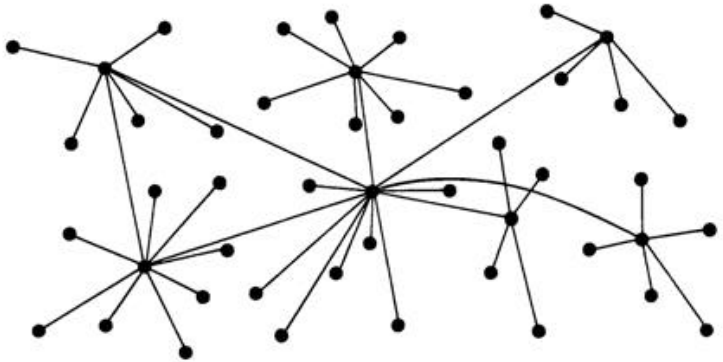
Lightning Network Payments Routing



Lightning Network Topology

What people think that network will look like

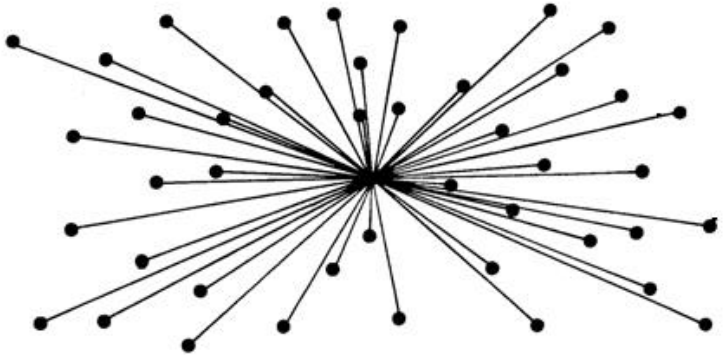




What Lightning Network will actually look like

Lightning Network Topology

What we had in fact



Offchain Settlement

BTC CHANNELS SNAPSHOT – 04 JUL 2017

Multisignature address	Client	Liquidity Hub
34i3ozADy8yknSPow4hfZevVUHE1gDEBMt	0.03073017	37.16926983
37zGsNecseFBYUEt2Q79vq5R4RJDsAjR7G	2.20091438	26.38003815
3GAkHd3dZhowFHqzQgmWGtCdKa1LDfQ9wT	6.75324318	22.24675682
35RgpgT11WJRW8vSqCTvny66eipGgYKWwz	2.53595479	17.46404521
3CN3UqxgZybCsEitdkMp8YUVmLaSweYvYH	0.00604847	14.99395153
…	…	…
3BFHeiYAo3BeGmzagQCzDobguVp7i6D5iR	0.00002917	0
3B73AV9i9EiVyuYYyTEWV55M3NfnTbjrpR	0.00002892	0
TOTAL in 2249 ‘BTC’ CHANNELS	**726.5220753**	**1104.964189**

Scaling settlement of Lykke trades

1. Only 20% trades triggers on-chain transactions. 80% trades are settled off-chain
2. Realtime settlement. Client has instant commitment even if it triggers on-chain transaction
3. No throughput limits

Costs growth

1. Client base growth
2. Number of active channels growth.
3. Fee rate growth
4. BTC price growth

Bitcoin Fees Jumps up

December 2017 switched to the centralized mode

1. 6 200 channels opened
2. 560 BTC frozen (8 mln USD)
3. 30 BTC fees takes to close channels (~400k USD)

Lightning Network Use Cases

1. Exchange-to-exchange transfers
2. Client buys coffee holding his BTC in hub’s custody (which is against decentralized idea)
3. ???

Let’s make Lykke decentralized again

Public Ledger is needed that would provide the following features

1. Handling up to 100k transactions per second
2. Sharding is required
3. Interoperability with other blockchains
4. Low fees